REMARKS

In the Office Action, the Examiner rejected claims 1-5 and 7-37, and objected to claim 6. By the present Response, Applicants have amended claims 1-6, 9-31, 33, and 35-36 and added new claims 38 and 39. These amendments do not add any new matter. Upon entry of these amendments, claims 1-39 will be pending in the present application and are believed to be in condition for allowance. In view of the foregoing amendments and the following remarks, Applicants respectfully request reconsideration and allowance of all pending claims.

Claim Rejections under 35 U.S.C. § 101

The Examiner rejected claims 13-20 under 35 U.S.C. § 101, because the claimed invention is directed to non-statutory subject matter. In particular, the Examiner stated that:

> [T]he claims are directed towards nonstatutory subject matter in the form of a computer program that is not claimed as embodied on a computer readable medium and executed by a computer system. The cited claims are an example of functional descriptive material consisting of data structures and programs that impart functionality when employed as executed by a computer component. The functionality of functional descriptive material is realized only when the functional descriptive material is claimed as being embodied on a computer readable medium and is claimed as executed by a computer component. The cited claims provide no tangible computer components that work in conjunction with the functional descriptive material to impart functionality and as a result the claims are not statutory because they fail the practical application requirement of § 101 by failing to provide a useful, concrete, and tangible result (see MPEP 2106).

Office Action, page 2. Applicants respectfully traverse this rejection.

Legal Precedent

Statutory subject matter, as set forth in Section 101, includes "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. As such, according to the Supreme Court, congress intended statutory subject matter to "include anything under the sun that is made by man." *Diamond v. Chakrabarty*, 447 U.S. 303, 308-09; 206 U.S.P.Q. 193, 197 (1980). In particular, it is clear that claims directed to products, apparatuses and devices are clearly statutorily patentable. As set forth in M.P.E.P § 2106(II)(c), "For products, the claim limitations will define discrete physical structures or materials. Product claims are claims that are directed to either machines, manufactures or compositions of matter."

Additionally, the Federal Circuit has developed a test which may be used to determine if a claim recites statutory subject matter, namely whether the claim produces a "useful, concrete, and tangible result." *In re Alappat*, 31 U.S.P.Q.2d 1545, 1557 (Fed. Cir. 1994) (*en banc*). The Federal Circuit has stated "the dispositive inquiry is whether the claim *as a whole* is directed to statutory subject matter." *Id.* The Federal Circuit elaborated by holding that one must look to "the essential characteristics of the subject matter, in particular, its practical utility." *State Street Bank & Trust Co. v. Signature Financial Group Inc.*, 47 U.S.P.Q.2d 1596, 1602 (Fed. Cir. 1998). Moreover, the Federal Circuit has stated "the *Alappat* inquiry simply requires an examination of the contested claims to see if the claimed subject matter *as a whole* is a disembodied mathematical concept representing nothing more than a 'law of nature' or an 'abstract idea,' or if the mathematical concept has been reduced to *some practical application rendering it 'useful'*." *AT&T Corp. v. Excel Communications, Inc.*, 50 U.S.P.Q.2d 1447, 1451 (Fed. Cir. 1999) (emphasis added). In other words, "Is an actual

process machine, manufacture, or composition of matter being claimed in accordance with 35 U.S.C. §101, or is the claim drawn to an abstraction?" Therefore, if a claim, read as a whole and in light of the specification, produces any useful, concrete, and tangible result, the claim meets the statutory requirements of Section 101. *See id*

Claims 13-20

Applicants respectfully assert that claims 13-20, as amended, are directed to statutory subject matter under Section 101, as they are directed to apparatuses and recite discrete physical structures. In particular, independent claim 13, is directed to "[a] first security module in a computer" and recites discrete physical structures. Specifically, the body of amended claim 13 recites "a *detector* that is adapted to determine if the first security module is a controlling security module or a subordinate security module . . . a *key generator* that generates a key . . . and a *key receiver* that receives a key . . ." (Emphasis added). (Emphasis added). Moreover, the specification clearly describes the security modules as including physical structure, stating that "[t]he TPMs 143 and 153 may include an input/output interface, a *processor*, and *memory*, routines, for example. These *various components* may be utilized to perform the functionality of the *detector* 82, the *key generator* 84, and the *key receiver* 86." Specification, paragraph 28, lines 3-6. (Emphasis added). Accordingly, the subject matter of independent claim 13 clearly contemplated to include *tangible* hardware elements, as well as software.

The Examiner's rejection seems based on a presumption that, because certain elements of the claimed invention may comprise software, that independent claim 13 and the claims dependent thereon, are non-statutory. This presumption is not correct. The

Commissioner of Patents has recognized the patentability of software, provided that it is embodied in a tangible medium. Indeed, the Commissioner has directly stated that, "computer programs embodied in a tangible medium...are patentable subject matter under 35 U.S.C. §101." *See In re Beauregard,* 53 F.3d 1583 (Fed Cir. 1995). It is *clear* from the specification that, to the extent the claimed security modules comprise software, the security modules are intended to be implemented in a tangible medium. In particular, the specification describes a first security module that includes NVRAM 140 (FIG. 3) and a second security module that includes a memory 160 (FIG. 3). Those of ordinary skill in the art would clearly recognize the NVRAM 140 and the memory 160 as tangible media. Because the specification clearly supports the software implementation of security modules in a tangible machine-readable medium, the Applicants' claims are statutory under the governing law of the Federal Circuit.

In summary, Applicants respectfully assert that claim 13, upon which claims 14-20 depend, is statutory because it is directed to either physical apparatuses or software that is stored on a tangible medium. As such, Applicants respectfully request withdrawal of the rejection of independent claim 13-20, under 35 U.S.C. § 101.

Claim Rejection Under 35 U.S.C. § 112, Second Paragraph

In the Office Action, the Examiner rejected claims 4-6, 8, 18, 22, 26 and 28 under 35 U.S.C. § 112, second paragraph, as being indefinite for "failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention." Office Action, page 3. Applicants respectfully traverse this rejection.

Legal Precedent and Guidelines

In ruling on a claim of patent indefiniteness, a court must determine whether those skilled in the art would understand what is claimed when the claim is read in light of the specification. *Personalized Media Communications, Inc. v. Int'l Trade Comm'n*, 161 F.3d 696, 705, 48 U.S.P.Q.2d 1880 (Fed. Cir. 1998); *Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1576, 1 U.S.P.Q.2d 1081 (Fed. Cir. 1986). A claim is not indefinite merely because it poses a difficult issue of claim construction; if the claim is subject to construction, i.e., it is not insolubly ambiguous, it is not invalid for indefiniteness. *Honeywell Int'l, Inc. v. Int'l Trade Comm'n*, 341 F.3d 1332, 1338-39, 68 U.S.P.Q.2d 1023 (Fed. Cir. 2003). That is, if the meaning of the claim is discernible, even though the task may be formidable and the conclusion may be one over which reasonable persons disagree, a claim is sufficiently clear to avoid invalidity on indefiniteness grounds. *Exxon Research & Eng'g Co. v. United States*, 265 F.3d 1371, 1375, 60 U.S.P.Q.2d 1272 (Fed. Cir. 2001). The failure to define a term is not fatal; if the meaning of the term is fairly inferable from the patent, an express definition is not necessary. *Bancorp Services LLC v. Hartford Life Insurance Co.*, 69 U.S.P.Q.2d 1996, 2000 (Fed. Cir. 2004). Even though an entire term is not defined in a patent or industry publications, individual components of the phrase may have well-recognized meanings to those of skill in art and a reader can infer the meaning of the entire phrase with reasonable confidence. *Id.*

Furthermore, the breadth of a claim is not to be equated with indefiniteness. *In re Miller*, 441 F.2d 689, 169 U.S.P.Q. 597 (CCPA 1971). In other words, a claim is not to be presumed indefinite merely because the claim includes a broad term. If the scope of the subject matter embraced by the claims is clear, and if Applicants have not otherwise indicated

that they intend the invention to be of a scope different from that defined in the claims, then the claims comply with 35 U.S.C. 112, second paragraph. *See* M.P.E.P. § 2173.04.

Claims 4-6, 18, 22, 28

The Examiner rejected claims 4-6, 18, 22 and 28 under 35 U.S.C. § 112. Specifically, the Examiner stated that:

> With regards to claim 4-6, 18, 22, 28, the limitation "measuring a system" is unclear because it is unclear what aspect of the system is being measured and what the system is.

Office Action, page 3. Applicants respectfully traverse this rejection. Although Applicants do not agree that the term "system" is ambiguous as recited in the claims at issue, in the interest of clarification, Applicants have amended claims 4-6, 18, 22, and 28 to recite "measuring a computer" instead of a "measuring a system." This amendment is not meant to narrow the scope of the original claim, but rather, to clarify features *already present* in the claims 4-6, 18, 22 and 28.

As set forth in Section 2173 of the Manual of Patent Examining Procedure, definiteness of claim language must be analyzed, not in a vacuum, but in light of:

> (A) The *content of the particular application disclosure*;
>
> (B) The teachings of the prior art; and
>
> (C) The *claim interpretation* that would be given by *one possessing the ordinary level of skill in the pertinent art* at the time the invention was made.

See M.P.E.P. § 2173.02. (Emphasis added). Applicants submit that one of ordinary skill in the art of security modules used in computing devices would understand "measuring" of a

computer to refer to the validation of various code and configurations in the computer for security purposes in order to determine integrity and build trust within the computer. Indeed, when reading the claims in view of the specification, it is clear that a security module uses keys to measure "*various code or configurations*, such as the BIOS 139 (FIG. 3), which may include *other system firmware*, and the *BIOS boot block*, if present. The measurement of a command or code may include cryptographically hashing the code to create integrity metrics." Specification, paragraph 31, lines 8-12. That the term "measuring" is broad enough to cover various types of actions does not render the claim indefinite. As such, the specification *clearly* supports and defines "measuring," as it used in the claims and Applicants assert that one of ordinary skill in the art would understand that the aspect being measured in claims 4-6, 18, 22, and 28 is the *overall security integrity of a computer*. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 4-6, 18, 22, and 28 under 35 U.S.C. § 112, second paragraph.

However, if the Examiner believes that a person of ordinary skill in the art having the benefit of the present disclosure would *not* understand "measuring a computer" as referring to obtaining an overall security measurement of a computer's integrity, Applicants respectfully request the Examiner explicitly set forth the level of skill attributed by the Examiner to a person of ordinary skill such that the person would *not* understand the meaning of the term "measure" in this context.

Claims 8 and 26

The Examiner also rejected claims 8 and 26 under 35 U.S.C. § 112. Specifically, the Examiner stated that:

> With regards to claims 8, 26, the claims define that the at least one key is comprised of two keys. It is unclear how a single key can be both a private key and a public key in a situation where there is only one key.

Office Action, page 3. Applicants respectfully traverse this rejection. Claims 8 and 26 recite "at least one key," referring to the ability of the security module taught by the present invention to generate either a single key or a *plurality* of keys. Indeed, the specification clearly states that the security module may generate and receive "a key *or keys*." Specification, paragraph 21, lines 8-11. (Emphasis added). Furthermore, the security module may generate a variety of different keys, including public keys, private keys, endorsement keys, and attestation identity keys. *See id.*, paragraph 29, lines 3-6. Thus, when read in view of the Specification, it is clear that "at least one key" encompasses embodiments of one key, more than one key and, furthermore, different key types. As such, Applicants respectfully assert that claims 8 and 26, reciting an embodiment where the "at least one key" comprises a private and a public key, is fully supported by the Specification and, moreover, would be understood by one of ordinary skill in the art. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 8 and 26 under 35 U.S.C. § 112, second paragraph.

Claim Rejections Under 35 U.S.C. § 102

In the Office Action, the Examiner rejected claims 31-32 under 35 U.S.C. § 102(e) as being anticipated by Challener, U.S. Patent No. 7,095,859 (hereafter referred to as "the Challener reference"). Applicants respectfully traverse this rejection.

Legal Precedent

Anticipation under Section 102 can be found only if a single reference shows exactly what is claimed. *See Titanium Metals Corp. v. Banner*, 227 U.S.P.Q. 773 (Fed. Cir.1985). For a prior art reference to anticipate under Section 102, every element of the claimed invention must be identically shown in a single reference. *See In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir.1990). That is, the prior art reference must show the *identical invention "in as complete detail as contained in the ... claim"* to support a *prima facie* case of anticipation. *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q. 2d 1913, 1920 (Fed. Cir. 1989) (emphasis added). Thus, for anticipation, the cited reference must not only disclose all of the recited features but must also disclose the *part-to-part relationships* between these features. *See Lindermann Maschinenfabrik GMBH v. American Hoist & Derrick*, 221 U.S.P.Q. 481, 486 (Fed. Cir.1984). Accordingly, the Applicants need only point to a single element or claimed relationship not found in the cited reference to demonstrate that the cited reference fails to anticipate the claimed subject matter. A *strict correspondence* between the claimed language and the cited reference must be established for a valid anticipation rejection.

Independent Claim 31

Applicants respectfully assert that the Challener reference does not anticipate independent claim 31. Amended independent claim 31 recites, "[a] method of initializing a plurality of security modules in *a computer*." (Emphasis added). In sharp contrast, the Challenger reference discloses modules being located in *two separate and distinct computers*, a client computer and a server computer. *See* Challener, Fig. 1; col. 3, lines 52-59. Furthermore, the Challener reference is absent of any language teaching or suggesting a

plurality of security modules in *a computer*. For at least this reason, the Challener reference cannot anticipate independent claim 31 or its dependent claims. Accordingly, Applicants respectfully request withdrawal of the rejection under 35 U.S.C. § 102(e) and allowance of claims 31 and 32.

Claim Rejections Under 35 U.S.C. § 103(a)

In the Office Action, the Examiner rejected claims 1-5, 7-30, 33-34 and 36-37 under 35 U.S.C. § 103(a) as being unpatentable over the Challener reference in view of Williams, U.S. Patent No. 5,559,883 (hereafter referred to as "the Williams reference"); and rejected claim 35 under 35 U.S.C. § 103(a) as being unpatentable over the Challener reference in view of Zinsky et al., U.S. Patent No. 6,480,097 (hereafter referred to as "the Zinsky reference"). Applicants respectfully traverse these rejections.

Legal Precedent

The burden of establishing a *prima facie* case of obviousness falls on the Examiner. *Ex parte Wolters and Kuypers*, 214 U.S.P.Q. 735 (B.P.A.I. 1979). To establish a *prima facie* case, the Examiner must not only show that the combination includes *all* of the claimed elements, but also a convincing line of reason as to why one of ordinary skill in the art would have found the claimed invention to have been obvious in light of the teachings of the references. *Ex parte Clapp*, 227 U.S.P.Q. 972 (B.P.A.I. 1985). In establishing a *prima facie* case for obviousness, "the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or

nonobviousness of the subject matter is determined." *KSR Int'l Co. v. Teleflex, Inc.*, 127 S. Ct. 1727 at 1729 (2007).

Independent Claims 1, 13, 21, 23 and 36

Applicants respectfully assert that several features of amended independent claims 1, 13, 21, 23, and 36 are not disclosed by either the Challener reference or the Williams reference. Independent claims 1, 13, 21, and 23, recite, *inter alia*, "a first security module *in a computer* . . .and . . . a second security module *within the computer*." (Emphasis added). Independent claim 36 recites, *inter alia*, "*one* of the plurality of computers *comprising* a first security module *and* a second security module." (Emphasis added). However, as discussed above, the Challenger reference discloses modules being located in *two separate and distinct computers*, for example, a client computer and a server computer. *See* Challener, Fig. 1; col. 3, lines 52-59. Further, while the Williams reference discloses a plurality of security modules, the security modules are deployed as part of a local area network (LAN) comprising of many computers. *See* Williams, Fig. 2; col. 2, lines 28-34. Client computers on the LAN connect to the security module, thus providing a *centralized* security architecture for the LAN. *See id.* However, Williams makes no teaching or suggestion that multiple security modules are located in a single computer. Accordingly, the Williams reference does not overcome the deficiencies of the Challener reference. For at least this reason, Applicants respectfully request withdrawal of the Section 103 rejection of claims 1, 13, 21, 23 and 36.

Moreover, Applicants believe that the Challener and Williams references are also deficient for additional reasons set forth below. Independent claims 1, 13, 21, 23, and 36 further recite that a security module taught by the present invention has a mechanism for

determining whether it is controlling or subordinate with respect to other security modules. Specifically, independent claim 1 recites, *inter alia*, "initializing a first security module, the method comprising . . . determining if the first security module is a controlling security module." (Emphasis added). Independent claim 13 recites "a first security module *comprising . . . a detector* that is adapted to *determine* if the first security module is a controlling security module or a subordinate security module." (Emphasis added). Independent claim 21 recites a first security module *comprising . . . means for determining* if the first security module is a controlling security module or a subordinate security module." (Emphasis added). Independent claim 23 recites, *inter alia*, "first and second security modules being configured to *determine* whether the first security module or the second security module is a controlling security module or a subordinate security module." (Emphasis added). Independent claim 36 recites "a first security module and a second security module being configured to *determine* whether the first security module or the second security module is a controlling security module or a subordinate security module." (Emphasis added).

In the Office Action, the Examiner admits that the Challener reference does not disclose determining if a security module is a controlling module or a subordinate module. *See* Office Action, page 5. Furthermore, the security modules disclosed in the Williams reference make *no determination* as to whether they have primary (controlling) and secondary (subordinate) status. Instead, an *external* "management module" is relied upon for assigning primary (controlling) and secondary (subordinate) status to the security modules. *See* Williams, col. 11, lines 23-34. "Selection of the primary and standby security modules is *solely the responsibility of the management module 18*." *Id.* at col. 11, lines 28-29. It

appears that security modules themselves, as taught by the Williams reference, are *incapable* of making any determination as to their primary or secondary status. Instead, they must rely on instructions given by a separate and distinct *management module*, wherein "[t]he [security] module designated as primary server remains so until it either fails, or the *management module 18 instructs it to become a standby*." *Id.* at col. 11, lines 29-32. Indeed, it does not appear the Williams reference contains any language teaching or suggesting that the security modules comprise some *internal* mechanism for determining whether or not it is a controlling or a subordinate module. Moreover, the Challener reference does not cure the deficiencies of the Williams reference. In view of these deficiencies among others, the Challener and Williams references, taken alone or in hypothetical combination, cannot render obvious independent claims 1, 13, 21, 23, and 36. Applicants respectfully request withdrawal of the rejections of claims 1, 13, 21, 23, and 36 as well as the rejection of all claims depending therefrom, under 35 U.S.C. § 103(a).

Claims 33 and 34

Claims 33 and 34 depend from claim 31. As stated above, the Williams reference fails to obviate the deficiencies of the Challener reference because it does not teach or suggest "a plurality of security modules in *a computer*," as recited by independent claim 31. Accordingly, the Williams reference fails to overcome the deficiencies of the Challener reference with respect to claim 31 and Applicants respectfully request allowance of claims 33 and 34 based on the dependency.

Claim 35

Claim 35 depends from claim 31. The Examiner rejected claim 35 as being unpatentable over the Challener reference in view of the Zinsky reference. Zinsky discloses a computer having security features implemented in system ROM to provide a password at power-on to a security device controlling access to secured features. *See* Zinksy, col. 2, lines 13-16. However, the Zinksy reference does not teach or suggest "a plurality of security modules in *a computer*," as recited by independent claim 31. Accordingly, the Zinsky reference fails to overcome the deficiencies of the Challener reference with respect to claim 31 and Applicants respectfully request allowance of claim 35 based on the dependency.

Allowable Subject Matter

In the Office Action, the Examiner objected to claim 6 as being dependent upon a rejected base claim, but stated that claim 6 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Applicants would like to thank the Examiner for indicating the potential allowability of claim 6. At this time, however, the Applicants believe that all of the pending claims are allowable and have thus chosen not to rewrite claim 6 in independent form.

Payment of Fees and General Authorization for Extensions of Time

The Commissioner is authorized to charge the fee of $100.00 for additional claims to Deposit Account No. 08-2025. If any additional fees, including fees for extensions of time and other reasons, are deemed necessary to advance prosecution of the present application, at this or any other time, Applicants hereby authorize the Commissioner to charge such requisite fees to Deposit Account No. 08-2025; Order No. 200314542-1. In accordance with

37 C.F.R. § 1.136, Applicants hereby provide a general authorization to treat this and any future reply requiring an extension of time as incorporating a request thereof.

Conclusion

In view of the remarks and amendments set forth above, Applicants respectfully request allowance of the pending claims. If the Examiner believes that a telephonic interview will help speed this application toward issuance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Date: September 24, 2007

Michael G. Fletcher
Reg. No. 32,777
FLETCHER YODER
PO Box 692289
Houston, TX 77269-2289
(281) 970-4545

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Department, M/S 35
P.O. Box 272400
Fort Collins, Colorado 80527-2400